

## REMARKS

Claims 1-7 are pending. Claims 1, 3 and 5 have been amended. Claims 2 and 4 have been previously presented. Claims 6 and 7 are new. No new matter has been introduced by the amendment.

### 1. Double Patenting Rejections

Claims 1-4 have been rejected on the ground of non-statutory obviousness-type double patenting over claims 1-2 of U.S. Patent No. 7,002,449. The Applicant respectfully traverses these rejections based on the following remarks.

The Examiner has conceded that the following element recited in the instant claims, "an encryption unit for encrypting security data of the vehicle with a cipher key is interposed between the controller and the nonvolatile memory of the in-vehicle unit", is not disclosed in claims 1-2 of U.S. Patent No. 7,002,449 (Office Action, page 3). The Examiner nevertheless asserts that the instant claims are not patentably distinct from claims 1-2 of U.S. Patent No. 7,002,449 because it "would have been obvious to one having ordinary skill in the art to recognize that by encrypting the security data with a cipher key only authorized users can access the vehicle locking and unlocking mechanism thereby stopping any unauthorized access to the secure vehicle data" (Office Action, page 3).

Claims 1-4 of the present invention are characterized in encryption, whereas there is no disclosure in relation thereto in claims 1-2 of U.S. Patent No. 7,002,449. Claims 1-4 of the present invention are not such ones as recognized by the Examiner, that is, data is encrypted so that an authorized user has access to it. The Applicant thus respectfully submits that the Examiner incorrectly states that the conflicting claims are not patentably distinct from each other. Accordingly, the Applicant further

respectfully submits that the rejections on the ground of non-statutory obviousness-type double patenting against claims 1-4 are improper and should be withdrawn.

## **2. Drawings**

Figure 3 has been designated as "Prior Art" in the replacement sheet. Accordingly, the Applicant respectfully submits that the objection to the drawings has been overcome and should be withdrawn.

## **3. Claim Objections**

Claims 1 and 3 have been objected to because of informalities. Claim 3 has been amended as suggested by the Examiner. Independent claim 1 has been amended to clarify that encryption is performed at the time of ID registration to the in-vehicle unit. The "cipher key" as recited in amended independent claim 1 corresponds to the second cipher key in exemplary embodiments of the specification, rather than to the first cipher key in exemplary embodiments of the specification. Support for amended independent claim 1 can be found in Applicant's specification, for example, on page 10, lines 10-23. Accordingly, the Applicant respectfully submits that the objections to claims 1 and 3 have been overcome and should be withdrawn.

## **4. Claim Rejections under 35 U.S.C. § 112, First Paragraph**

Claims 1-5 have been rejected under 35 U.S.C. § 112, first paragraph. The Examiner asserts that "applicant does not include "a second cipher key" and "ID that is encrypted with the second cipher key" in the claims" (Office Action, page 6). As discussed above, independent claim 1 has been amended to clearly indicate that the "second cipher key" in exemplary embodiments of the specification corresponds to a cipher key at the time of registration, and thus the "cipher key" in amended independent claims 1 and 5. Accordingly, the Applicant respectfully submits that the

rejections under 35 U.S.C. § 112, first paragraph, have been overcome and should be withdrawn.

#### **5. Claim Rejections under 35 U.S.C. § 102(b) And New Claims**

Claims 1-5 have been rejected under 35 U.S.C. § 102(b) over Berra (U.S. Pat. No. 5,787,367). The Applicant respectfully traverses these rejections based on the following remarks.

Berra discloses a flash reprogrammable security for vehicle computer in which the “authorized database 30 includes an encryption device such as encryption software for encrypting data that is transmitted from the authorized database 30 to remote devices through modem 32” (column 4, lines 37-50). Berra, however, does not disclose, except that the data is read out from the authorized database 30, that the data is registered therein. It follows that Berra does not disclose that the data is put into a register mode. Nor is there any disclosure in Berra regarding what kind of memory the register memory is. It is further noted that Berra merely discloses that EEPROM (40) is provided in the engine control unit (12) (column 4, lines 54-60). Berra does not disclose any EEPROM (40) in relation to encryption.

In contrast, the handling device of security data recited in amended independent claim 1 comprises an in-vehicle unit having a portable unit authenticating unit, a nonvolatile memory, and a controller, and a vehicle having the in-vehicle unit, an in-vehicle system, and a communication unit, wherein the portable unit transmits a signal indicating the ID of the portable unit to the vehicle, the communication unit receives the transmission signal, the portable unit authenticating unit authenticates as to whether the signal is a transmission signal that is transmitted from a predetermined portable unit based on a comparison between the reception

signal and data indicating the ID of the portable unit stored in the nonvolatile memory or not, the control unit causes the in-vehicle system to perform the control instructions if the portable unit authenticating unit judges that the signal is a transmission signal that is transmitted from a predetermined portable unit, an encryption unit for encrypting security data of the vehicle with a cipher key is interposed between the controller and the nonvolatile memory of the in-vehicle unit, and the security data is encrypted with the cipher key and stored into the nonvolatile memory according to the instruction from the controller when the in-vehicle unit is set into a security data register mode.

The handling method of security data of a vehicle recited in amended independent claim 5 comprises transmitting, from the portable unit, instructions for locking/ unlocking the door locking mechanism of the vehicle and a signal indicating the ID of the portable unit; receiving the signal by the communication unit provided in the vehicle; the portable unit authenticating unit authenticating as to whether the signal is a transmission signal that is transmitted from a predetermined portable unit based on a comparison between data indicating the ID of the portable unit stored in the nonvolatile memory and data indicating the ID of the portable unit contained in the signal transmitted from the portable unit or not; the control unit provided in the in-vehicle unit causing the door lock mechanism to be locked/unlocked if the portable unit authenticating unit judges that the signal is a transmission signal that is transmitted from a predetermined portable unit; encrypting the security data with a cipher key in an encryption unit provided between the controller and the first nonvolatile memory of the in-vehicle unit; and storing the encrypted signal into the first nonvolatile memory and storing the cipher key into a second nonvolatile memory, wherein an encryption unit for encrypting the ID of the portable unit with a cipher key is interposed between the controller and the nonvolatile memory of the in-

vehicle unit, and the ID of the portable unit contained in the signal transmitted from the portable unit is encrypted with the cipher key and stored into the nonvolatile memory according to the instruction from the controller when the transmission signal is received from the portable unit after setting the in-vehicle unit into an ID register mode. Support for amended independent claims 1 and 5 can be found in Applicant's specification, for example, on page 8, line 9 to page 10, line 23, and in Figs. 1 and 2.

As described above, the feature of the present invention as recited in the amended independent claims 1 and 5, that is, encrypted data is registered at the time of registration into a nonvolatile memory in a register mode, is not disclosed nor suggested in Berra. With such a feature, the present invention offers an advantageous effect as described in the specification as originally filed. In contrast, the cited invention does not offer such an advantageous effect.

In view of the above amendments and remarks, the Applicants respectfully submit that Berra does not teach or suggest all the claim limitations as recited in amended independent claims 1 and 5. Accordingly, the rejections against amended independent claims 1 and 5, and thus the rejections against claims 2-4 and 6-7, which all depend from amended independent claim 1, have been overcome and should be withdrawn. Support for new claims 6-7 can be found in Applicant's specification, for example, on page 11, lines 8-10 and on page 10, lines 10-23.

Application No. 10/687,311

Amendment in Response to Non-Final Office Action Mailed March 7, 2007

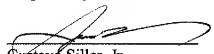
Page 11 of 11

## 6. Conclusion

Based on the above amendments and remarks, the Applicant respectfully submits that the claims are in condition for allowance. The examiner is kindly invited to contact the undersigned attorney to expedite allowance.

Respectfully submitted,

Date: June 5, 2007

  
Gustavo Siller, Jr.  
Registration No. 32,305  
Attorney for Applicant

BRINKS HOFER GILSON & LIONE  
P.O. BOX 10395  
CHICAGO, IL 60610  
(312) 321-4200